Billing Code

DEPARTMENT OF DEFENSE

Office of the Secretary

[Docket ID DoD-2022-OS-0065]

Privacy Act of 1974; System of Records

AGENCY: Office of the Secretary, Department of Defense (DoD).

ACTION: Notice of a new system of records.

SUMMARY: In accordance with the Privacy Act of 1974, the Department of Defense (DoD) is establishing a new Department-wide system of records titled, "Counterintelligence Functional Services," DoD-0010. This system of records covers DoD's maintenance of records about counterintelligence functional services (CIFS). The purpose of CIFS is to protect Department resources and personnel from foreign adversaries who seek to exploit sensitive information, operations, and agency programs to the detriment of the U.S. Government. The DoD is issuing a Notice of Proposed Rulemaking, which proposes to exempt this system of records from certain provisions of the Privacy Act, elsewhere in today's issue of the *Federal Register*.

DATES: This system of records is effective upon publication; however, comments on the Routine Uses will be accepted on or before [INSERT DATE 30 DAYS AFTER DATE OF PUBLICATION IN THE FEDERAL REGISTER]. The Routine Uses are effective at the close of the comment period.

ADDRESSES: You may submit comments, identified by docket number and title, by any of the following methods:

* Federal Rulemaking Portal: https://www.regulations.gov.

Follow the instructions for submitting comments.

* Mail: Department of Defense, Office of the Assistant to the Secretary of Defense for Privacy, Civil Liberties, and Transparency, Regulatory Directorate, 4800 Mark Center Drive, Attn: Mailbox 24, Suite 08D09, Alexandria, VA 22350-1700.

Instructions: All submissions received must include the agency name and docket number for this *Federal Register* document. The general policy for comments and other submissions from members of the public is to make these submissions available for public viewing on the Internet at https://www.regulations.gov as they are received without change, including any personal identifiers or contact information.

FOR FURTHER INFORMATION CONTACT: Ms. Rahwa Keleta, Privacy and Civil Liberties Division, Directorate for Privacy, Civil Liberties and Freedom of Information, Office of the Assistant to the Secretary of Defense for Privacy, Civil Liberties, and Transparency, Department of Defense, 4800 Mark Center Drive, Mailbox #24, Suite 08D09, Alexandria, VA 22350-1700; OSD.DPCLTD@mail.mil; (703) 571-0070.

SUPPLEMENTARY INFORMATION:

I. Background

DoD is establishing "Counterintelligence Functions Services (CIFS)," DoD-0010, as a DoD-wide Privacy Act system of records. A DoD-wide System of Records Notice (SORN) supports multiple DoD paper or electronic recordkeeping systems operated by more than one DoD component that maintain the same kind of information about individuals for the same purpose. Establishment of DoD-wide SORNs helps DoD standardize the rules governing the collection, maintenance, use, and sharing of personal information in key areas across the enterprise. DoD-wide SORNs also reduce duplicative and overlapping SORNs published by separate DoD components. The creation of DoD-wide SORNs is expected to make locating relevant SORNs easier for DoD personnel and the public, and create efficiencies in the operation of the DoD privacy program.

The Counterintelligence (CI) mission is critical to the protection of DoD personnel, installations, and activities; the Defense Industrial Base (DIB); and the National Industrial Security Program (NISP). To further this mission, the Department is authorized to gather individuals' information to protect against espionage, intelligence activities, sabotage, or

assassinations conducted by foreign entities or international terrorists. CIFS activities include support to the following CI missions: counter-espionage; international terrorism; and support to force protection, research, development, and acquisition. CIFS also include CI incident assessments and required CI reporting that is conducted throughout DoD. CI activities not covered under this SORN are CI investigations and CI collection activities; those activities are conducted within the Department solely by the Military Department Counterintelligence Organizations (MDCOs). The CIFS SORN records contain information on both Federal employees, uniformed service members, contractors, and members of the public. The CIFS system of records contains data derived from government records (Federal, state, and local) and information collected directly from the public.

Additionally, DoD is issuing a Notice of Proposed Rulemaking to exempt this system of records from certain provisions of the Privacy Act elsewhere in today's issue of the *Federal Register*.

II. Privacy Act

Under the Privacy Act, a "system of records" is a group of records under the control of an agency from which information is retrieved by the name of an individual or by some identifying number, symbol, or other identifying particular assigned to the individual. In the Privacy Act, an individual is defined as a U.S. citizen or lawful permanent resident.

In accordance with 5 U.S.C. 552a(r) and Office of Management and Budget (OMB) Circular No. A-108, DoD has provided a report of this system of records to the OMB and to Congress.

Dated: June 21, 2022.

Aaron T. Siegel,

Alternate OSD Federal Register

Liaison Officer, Department of Defense.

SYSTEM NAME AND NUMBER: "Counterintelligence Functional Services (CIFS)," DoD-0010.

SECURITY CLASSIFICATION: Unclassified; Classified.

SYSTEM LOCATION:

A. Department of Defense (Department or DoD), located at 1000 Defense Pentagon, Washington, D.C. 20301-1000, and other Department installations, offices, or mission locations.

B. Information may also be stored within a government-certified cloud, implemented and overseen by the Department's Chief Information Officer (CIO), 6000 Defense Pentagon, Washington, D.C. 20301-6000.

SYSTEM MANAGER(S):

A. Director for Defense Counterintelligence, Law Enforcement & Security, Office of the Under Secretary of Defense for Intelligence & Security, 1000 Defense, Pentagon, Washington, D.C. 20301-1100 who is also responsible for implementing policy for the CIFS program within DoD.

B. The three Military Department Counterintelligence Organizations (MDCOs): Air Force Office of Special Investigations (AFOSI), Naval Criminal Investigation Services (NCIS), and U.S. Army Intelligence and Security Command (INSCOM), each of which supports certain Department components in the operation of the CIFS program. Department components are assigned to and supported by the three MDCOs; or through their designated units. Although AFOSI, NCIS and INSCOM may conduct CIFS on behalf of units assigned to them, most CIFS activities are conducted by the components themselves with support by the MDCOs. DoD components include the Military Departments of the Army, Air Force (including the U.S. Space Force), and Navy (including the U.S. Marine Corps), field operating agencies, major commands, field commands, installations, and activities. To contact the system manager at the DoD

component with oversight of the records, go to www.FOIA.gov to locate the contact information for each component's Freedom of Information Act (FOIA) office.

AUTHORITY FOR MAINTENANCE OF THE SYSTEM: National Security Agency Act of 1959, as amended (Pub. L. 86-36) (codified at 50 U.S.C. 3601 et seq.); the Foreign Intelligence Surveillance Act (FISA), as amended (Pub. L. 95-511) (codified at 50 U.S.C. 1801 et seq.); 44 U.S.C. Subchapter II (3551-3559), Information Security (Federal Information Security Modernization Act of 2014 (FISMA); 50 U.S.C. 3381, Coordination of Counterintelligence Activities; Executive Order (E.O.) 12333, as amended, United States intelligence activities; E.O. 13526, Classified National Security Information; National Security Directive 42, National Policy for the Security of National Security Telecommunications and Information Systems; E.O. 9397 (SSN), as amended by E.O. 13478.

PURPOSE(S) OF THE SYSTEM:

A. To manage the CI Awareness and Reporting program; provide briefings on concerns of treason, spying, espionage, sabotage, terrorism, subversion, sedition, and other suspicious matters of related CI interest for threat identification and mitigation.

B. To provide CI support (such as information collection, records review and agency coordination) to assess threats against DoD operations, data, personnel, facilities, and systems. CI support is integrated into all DoD missions, specifically including the following mission areas and programs: arms control and other international weapons treaties; counter-proliferation and countering weapons of mass destruction; DoD foreign visitors program and foreign personnel exchange programs; counterintelligence screening of military applicants; DoD antiterrorism and force protection programs; military operations and exercises; cyber operations; DoD insider threat program; critical infrastructure protection; operations security programs; research, development, and acquisition programs; and other defense and national security activities as assigned to the DoD in accordance with applicable law and policy.

C. To conduct CI Incident Assessments; examine information of CI interest and determine whether a CI investigation may be warranted; liaise, conduct coordination and de-conflict assessments with intelligence, security, military, and law enforcement (LE) agencies in the area of operations.

D. To conduct specialized technical services such as analysis of information technology from auditing and monitoring for systems; provide polygraph and credibility assessment support, surveillance and technical surveillance countermeasures (TSCM) activities, and digital and biometric forensics activities.

CATEGORIES OF INDIVIDUALS COVERED BY THE SYSTEM: Individuals involved in, mentioned in, and/or subject to CI reporting requirements or CI incident assessments; individuals to whom reporting pertains; individuals within DoD's investigatory jurisdiction, including military and civilian employees or individuals employed by contractors. Records may also include information about other types of individuals not covered by the system, such as complainants, sources, subjects, and witnesses.

CATEGORIES OF RECORDS IN THE SYSTEM: CIFS records include CI awareness and reporting records, threat assessment records, incident assessment records, and records produced as a result of CI specialized technical services. These records may contain the following data elements as necessary.

A. Personal information such as: names, social security numbers, DoD/ID numbers, employee identification numbers, date and place of birth, addresses, contact information; biometric information, fingerprints and retinal data; medical/psychological information; travel identification information (passport, visa, resident alien), driver's license information (state, number, and expiration date, etc.); biographic information, family and dependent information; gender, race/ethnicity, and property information.

B. Employment Information such as: position/title, rank/grade, duty station; work address, e-mail address, supervisor's name and contact information; military records, personnel security

information, employment personnel files, financial information (to include tax identification information), financial reports and transaction data; and education and training records.

Note: This system of records does not encompass records collected, used, and maintained for CI investigations or CI collection activities.

RECORD SOURCE CATEGORIES: Records and information stored in this system of records are obtained from: Individuals, government sources (Federal, state, local, tribal and foreign), social media, periodicals, newspapers, information from commercial databases; and information from classified sources to include intelligence reports, security sources, law enforcement information, and correspondence.

ROUTINE USES OF RECORDS MAINTAINED IN THE SYSTEM, INCLUDING CATEGORIES OF USERS AND PURPOSES OF SUCH USES: In addition to those disclosures generally permitted under 5 U.S.C. 552a(b) of the Privacy Act of 1974, as amended, all or a portion of the records or information contained herein may specifically be disclosed outside the DoD as a Routine Use pursuant to 5 U.S.C. 552a(b)(3) as follows:

A. To contractors, grantees, experts, consultants, students, and others performing or working on a contract, service, grant, cooperative agreement, or other assignment for the federal government when necessary to accomplish an agency function related to this system of records.

B. To the appropriate Federal, State, local, territorial, tribal, foreign, or international law enforcement authority or other appropriate entity where a record, either alone or in conjunction with other information, indicates a violation or potential violation of law, whether criminal, civil, or regulatory in nature.

C. To any component of the Department of Justice for the purpose of representing the DoD, or its components, officers, employees, or members in pending or potential litigation to which the record is pertinent.

D. In an appropriate proceeding before a court, grand jury, or administrative or adjudicative body or official, when the DoD or other Agency representing the DoD determines that the

records are relevant and necessary to the proceeding; or in an appropriate proceeding before an administrative or adjudicative body when the adjudicator determines the records to be relevant to the proceeding.

E. To the National Archives and Records Administration for the purpose of records management inspections conducted under the authority of 44 U.S.C. 2904 and 2906.

F. To a Member of Congress or staff acting upon the Member's behalf when the Member or staff requests the information on behalf of, and at the request of, the individual who is the subject of the record.

G. To appropriate agencies, entities, and persons when (1) the DoD suspects or confirms a breach of the system of records; (2) the DoD determines as a result of the suspected or confirmed breach there is a risk of harm to individuals, the DoD (including its information systems, programs, and operations), the Federal Government, or national security; and (3) the disclosure made to such agencies, entities, and persons is reasonably necessary to assist in connection with the DoD's efforts to respond to the suspected or confirmed breach or to prevent, minimize, or remedy such harm.

H. To another Federal agency or Federal entity, when the DoD determines that information from this system of records is reasonably necessary to assist the recipient agency or entity in (1) responding to a suspected or confirmed breach or (2) preventing, minimizing, or remedying the risk of harm to individuals, the recipient agency or entity (including its information systems, programs and operations), the Federal Government, or national security, resulting from a suspected or confirmed breach.

I. To another Federal, State or local agency for the purpose of comparing to the agency's system of records or to non-Federal records, in coordination with an Office of Inspector General in conducting an audit, investigation, inspection, evaluation, or other review as authorized by the Inspector General Act.

J. To such recipients and under such circumstances and procedures as are mandated by Federal statute, treaty, or authorized mission.

K. To third parties during the course of an authorized inquiry to the extent necessary to obtain information pertinent to the inquiry, provided disclosure is appropriate to the proper performance of the official duties of the DoD official making the disclosure.

L. To U.S. Government officials for the purpose of addressing compromises of classified information including the information compromised, implications of disclosure of intelligence sources and methods, investigative data on compromises, and statistical and substantive analysis of the data.

M. To U.S. Government agencies or organizations for the purpose of performing audit or oversight operations as authorized by law or executive order, but only such information as is necessary and relevant to such audit or oversight function.

N. To appropriate Federal, state, local, territorial, tribal, foreign or international agencies having jurisdiction over the substance of the allegations or a related investigative interest in criminal law enforcement investigations, including statutory violations, counter-intelligence, counter-espionage and counter-terrorist activities and other security matters for the purpose of executing or enforcing laws designed to protect the national security or homeland security of the United States, to include activities described in 6 U.S.C. 485(a)(5), Domestic Security; 6 U.S.C. 482, Facilitating homeland security information sharing procedures; Intelligence Reform and Terrorism Protection Act of 2004; and E.O. 13388, Further Strengthening the Sharing of Terrorism Information to Protect Americans.

O. To designated officers, contractors, and employees of Federal, state, local, territorial, tribal, international, or foreign agencies for the purpose of the hiring, detailing, liaising, or retention of an individual, the conduct of a suitability or security investigation, the letting of a contract, or the issuance of a license, grant or other benefit, to the extent that the information is relevant and necessary to the agency's decision on the matter and that the employer is

appropriately informed about information that relates to or may impact an individual's suitability or eligibility.

P. To Federal and foreign government intelligence or counterterrorism agencies or components when DoD becomes aware of an indication of a threat or potential threat to national or international security, or when such use is to assist in anti-terrorism efforts and disclosure is appropriate to the proper performance of the official duties of the person making the disclosure.

Q. To a criminal, civil, or regulatory law enforcement authority (whether Federal, state, local, territorial, tribal, international, or foreign) when the information is necessary for collaboration, coordination, and de-confliction of investigative matters, to avoid duplicative or disruptive efforts, and for the safety of officers who may be working on related investigations.

R. To a court, magistrate, or administrative tribunal in the course of presenting evidence, including disclosures to opposing counsel or witnesses in the course of civil discovery, litigation, or settlement negotiations in response to a subpoena from a court of competent jurisdiction.

S. To a court, prosecutor, and/or defense attorney in satisfaction of the agency's obligations under the Jencks Act, 18 U.S.C. 3500; *Giglio v. United States*, 405 U.S. 150 (1972); or *Brady v. Maryland*, 373 U.S. 83 (1963).

POLICIES AND PRACTICES FOR STORAGE OF RECORDS: Records may be stored electronically or on paper in secure facilities in a locked drawer behind a locked door. Electronic records may be stored locally on digital media; in agency-owned cloud environments; or in vendor Cloud Service Offerings certified under the Federal Risk and Authorization Management Program (FedRAMP).

POLICIES AND PRACTICES FOR RETRIEVAL OF RECORDS: Records may be retrieved by personal and employment data elements that may identify the individual to whom the reporting pertains, including, but not limited to, name, social security number, DoD/ID or employment identification number, and email address.

POLICIES AND PRACTICES FOR RETENTION AND DISPOSAL OF RECORDS:

Records are maintained and disposed of in accordance with National Archives and Records Administration Schedules and authorized DoD Component Records Disposition Schedules. The retention period for specific records may be obtained by contacting the system manager for the Component.

ADMINISTRATIVE, TECHNICAL, AND PHYSICAL SAFEGUARDS: DoD safeguards records in this system of records according to applicable rules, policies, and procedures, including all applicable DoD automated systems security and access policies. DoD policies require the use of controls to minimize the risk of compromise of personally identifiable information (PII) in paper and electronic form and to enforce access by those with a need to know and with appropriate clearances. Additionally, DoD has established security audit and accountability policies and procedures which support the safeguarding of PII and detection of potential PII incidents. DoD routinely employs safeguards such as the following to information systems and paper recordkeeping systems: Multifactor log-in authentication including Common Access Card (CAC) authentication and password; physical token as required; physical and technological access controls governing access to data; network encryption to protect data transmitted over the network; disk encryption securing disks storing data; key management services to safeguard encryption keys; masking of sensitive data as practicable; mandatory information assurance and privacy training for individuals who will have access; identification, marking, and safeguarding of PII; physical access safeguards including multifactor identification physical access controls, detection and electronic alert systems for access to servers and other network infrastructure; and electronic intrusion detection systems in DoD facilities.

RECORD ACCESS PROCEDURES: Individuals seeking access to their records should follow the procedures in 32 CFR part 310. Individuals should address written inquiries to the DoD office with oversight of the records, as the component has Privacy Act responsibilities concerning access, amendment, and disclosure of the records within this system of records. The public may identify the contact information for the appropriate DoD office through the following

website: www.FOIA.gov. Signed written requests should contain the name and number of this system of records notice along with the full name, current address, and email address of the individual. Please provide additional identifying information for the records, if relevant, DoD ID Number or Defense Benefits Number, date of birth, and telephone number of the individual. In addition, the requester must provide either a notarized statement or an unsworn declaration made in accordance with 28 U.S.C. 1746, in the appropriate format:

If executed outside the United States: "I declare (or certify, verify, or state) under penalty of perjury under the laws of the United States of America that the foregoing is true and correct. Executed on (date). (Signature)."

If executed within the United States, its territories, possessions, or commonwealths: "I declare (or certify, verify, or state) under penalty of perjury that the foregoing is true and correct. Executed on (date). (Signature)."

CONTESTING RECORD PROCEDURES: Individuals seeking to amend or correct the content of records about them should follow the procedures in 32 CFR part 310.

NOTIFICATION PROCEDURES: Individuals seeking to determine whether information about themselves is contained in this system of records should follow the instructions for Record Access Procedures above.

EXEMPTIONS PROMULGATED FOR THE SYSTEM: DoD has exempted records maintained in this system from 5 U.S.C. 552a(c)(3); (d)(1), (2), (3) and (4); (e)(1); (e)(4)(G), (H) and (I); and (f) of the Privacy Act, pursuant to 5 U.S.C. 552a(k)(1), (k)(2), and (k)(5), as applicable. An exemption rule for this system has been promulgated in accordance with the requirements of 5 U.S.C. 553(b)(1), (2), and (3), (c), and (e) and published in 32 CFR part 310. In addition, when exempt records received from other systems of records become part of this system, DoD also claims the same exemptions for those records that are claimed for the prior system(s) of records of which they were a part, and claims any additional exemptions set forth here.

HISTORY: None

[FR Doc. 2022-13573 Filed: 6/23/2022 8:45 am; Publication Date: 6/24/2022]